Malware Detection using Malware Image and Deep Learning

Sunoh Choi, Sungwook Jang, Youngsoo Kim, Jonghyun Kim
Information Security Division
ETRI
Daejeon, South Korea
suno@etri.re.kr

***Abstract*—These days a lot of malware are generated. In order to deal with the new malware, we need new ways to detect malware. In this paper, we introduce a method to detect malware using deep learning. First, we generate images from benign files and malware. Second, by using deep learning, we train a model to detect malware. Then, by the trained model, we detect malware. By using malware images and deep learning, we can detect malware fast since we do not need any static analysis or dynamic analysis.**

Keywords—Malware Detection, Deep Learning

I. INTRODUCTION

PandaLabs reported that 27% of all malware which were detected by their antivirus engine were newly discovered in 2015 [7]. Every year a lot of new malware are created. It is very important to automate the process to detect the new malware. Recently automating to detect malware by using deep learning is widely researched.

Nowadays deep learning is widely used in various research areas. Especially it shows good results in image recognition [8]. Deep learning model has an input layer and an output layer and several hidden layers. When the deep learning model is trained with training data, it can automatically extract features and classify the data into several classes. For example, if the purpose of a deep learning model is image recognition, it can classify the images into several image classes. (e.g., dog, cat, flower, and so on)

In order to detect or classify malware, deep learning can be used. In order to use deep learning, we need training data of malware. There are three types of data. First is application program interface (API) sequences (e.g., CreateProcess) [9, 10, 11]. By running malware, we can get the API sequences. However, it takes quite a long time to run malware and get the API sequence. Second is opcode sequences [4]. We can get opcode sequences from the assembly codes of malware (e.g., MOV, ADD, and so on) Third is malware images [3,4]. We can make gray scale images from malware. In this paper, we focus on malware images to detect malware.

In Section II, we will show how to get malware images from malware. In Section III, we introduce a deep learning model which detects malware by using the malware images. Finally, in Section IV, we give the experimental results.

II. MALWARE IMAGES

In order to detect malware, we can make images from benign files and malware. This idea is from [1]. The idea is that a variant of malware have similar image and different malware have different image. In [1], they extracted pattern features from the images using GIST [2]. After that, they used k nearest neighbor (kNN) to classify malware. On the other hand, [3,4] make images and use deep learning to classify malware. But, in this paper, we make image and use deep learning to detect malware.

We make gray images from the files. In a gray image each pixel has a value from 0 to 255. When we make a gray image from a file, we read every 8 bits and convert it to an integer corresponding to a pixel. Then, we get a 256x256 image. The image size is 64KB. When the file is greater than 64KB, the remainder is discarded. When it is less than 64KB, the remainder of the image is padded with zero. In addition, when we use 256x256 images in deep learning, it runs out of memory. So, we down-sample the images to 32x32 images.

We can get images from the files fast compared to get API sequences. In order to get API sequences, we have to run each file for several minutes. In order to prevent malware from running in real-time, we have to check whether the file is malicious or not within several seconds. So, we believe that for the malware detection, getting malware image is much better than extracting the API sequences.

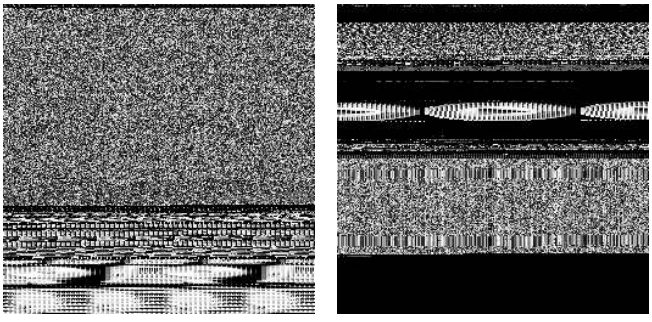

Fig. 1. Normal File Image (left) and Malware Image (right)

III. Malware Detection using Deep Learning

In this section, we introduce a deep learning model for malware detection using malware image. Deep learning is widely used in image recognition. Especially convolutional neural network (CNN) is mainly used. In neural network, each node in the previous layer gives effects to all nodes in the next layer. However, in CNN, only several nodes in the current layer give effects to the nodes in the next layer. So, CNNs are able to use local correlation. It means that CNN learns features from the images.

Fig. 2 shows our deep learning model. It has three convolutional layers followed by a pooling layer respectively and two fully connected layers. By using the pooling layer, the deep learning model is robust to the small changes in the images.

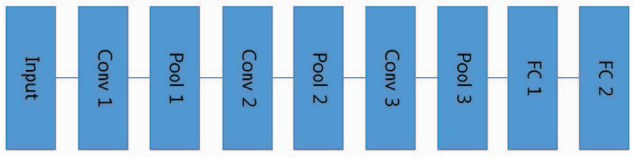

Fig. 2. Deep Learning Model

IV. Experimental Results

We implemented a preprocessing module to make images from benign files and malware and a deep learning module shown in Fig 3. We used a machine having Nvidia GPU 1060 running Ubuntu 14.04, python 3.4.3 and cuda 8.0 to measure the accuracy of our malware detection system.

We get 10,000 normal files from Hauri [5] which is a Korea antivirus company and 2,000 malware from Kaist Cyber Security Research Center [6]. 90% of the files are used for training and 10% are used for test.

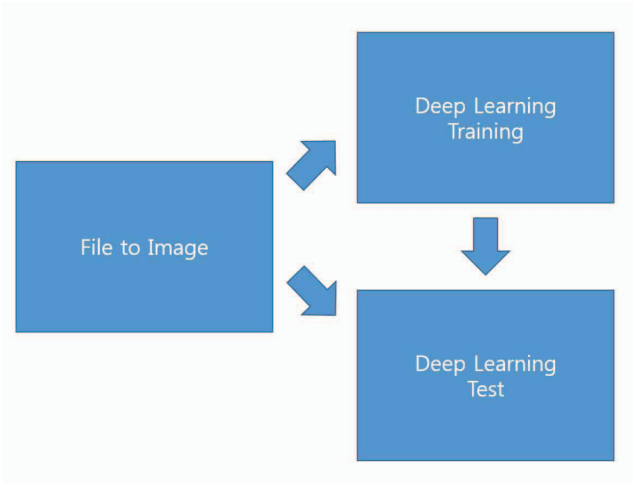

Fig. 3. Malware Detection System

Fig. 4 shows the accuracy of our malware detection system. The accuracy is defined as follows.

$$\text{Accuracy} = (TP+TN) / (TP+FP+FN+TN)$$

where TP is the number of things which are real malware and are predicted as malware and TN is the number of things which are real benign files and are predicted as a benign files and FP is the number of things which are real benign files but predicted as malware and FN is the number of things which are real malware but predicted as benign files.

The number of malware is fixed as 2,000 in our experiment and the number of benign files increases from 2,000 to 10,000. When there are 10,000 normal files and 2,000 malware, the accuracy is 0.9566. This is our preliminary result. In the future, we will use more malware and develop various deep learning models. Then, we expect that we can get higher accuracy.

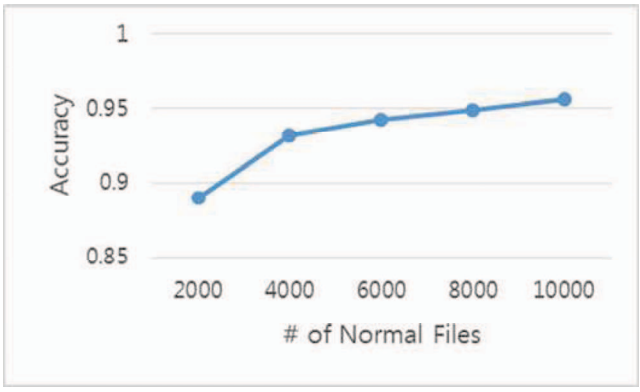

Fig. 4. Accuracy

V. Conclusions

In this paper, we introduce a method to detect malware using malware image and deep learning. First, we generate images from benign files and malware since a variant of malware has a similar image with the malware. In addition, we can get the images fast compared to API sequences. Second, by using deep learning model based on CNN, we detect malware since CNN model learns features from the images. In our preliminary experimental results, the accuracy is about 96%. In the future, we will use other preprocessing methods to detect malware as well as malware images. We can use API system call sequences by doing dynamic analysis or use opcodes by doing static analysis.

Acknowledgment

This work was supported by Institute for Information & communications Technology Promotion(IITP) grant funded by the Korea government(MSIT) (No.2016-0-00078, Cloud based Security Intelligence Technology Development for the Customized Security Service Provisioning)

REFERENCES

[1] L. Nataraj, S. Karthikeyan, G. Jacob, and B. S. Manjunath, Malware Images: Virualization and Automatic Classification, ACM VizSec, 2011

[2] Oliva, A. and Torralba, A., Modeling the shape of a scene: a holistic representation of the spatial envelope, International Journal of Computer Vision, 2001

[3] Seonhee Seok and Howon Kim, Visualized Malware Classification Based on Convolutional Neural Network, Journal of The Korea Institute of Information Security and Cryptology, 2016

[4] Daniel Gibert, Convolutional Neural Networks for Malware Classification, Master Thesis, Unisersitat Politecnica de Catalunya, 2016

[5] Hauri, https://www.hauri.co.kr

[6] Kaist Cyber Security Research Center, http://csrc.kaist.ac.kr

[7] Panda, http://www.pandasecurity.com/mediacenter/press-releases/all-recorded-malware-appeared-in-2015/

[8] Alex Krizhevsky, Ilya Sutskever, and Geoffrey E. Hinton, ImageNet Classification with Deep Convolutional Neural Networks, International Conference on Neural Information Processing Systems (NIPS), 2012

[9] George E. Dahl, Jack W. Stokes, Li Deng, and Dong Yu, Large-Scale Malware Classification using Random Projections and Neural Networks, IEEE ICASSP, 2013

[10] Razvan Pascanu, Jack W. Stokes, Hermineh Sanossian, Mady Marinescu, and Anil Thomas, Malware Classification with Recurrent Networks, IEEE ICASSP, 2015

[11] Wenyi Huang and Jack W. Stokes, MtNet: A Multi-Task Neural Network for Dynamic Malware Classification, DIMVA, 2016